UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/542,500	07/15/2005	Gerfried Ranner	282594US8XPCT	5322

22850 7590 06/06/2007	**EXAMINER**
OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.	CHAI, LONGBIT
1940 DUKE STREET	
ALEXANDRIA, VA 22314	

ART UNIT	PAPER NUMBER
2131	

NOTIFICATION DATE	DELIVERY MODE
06/06/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/542,500	RANNER ET AL.
	Examiner	**Art Unit**
	Longbit Chai	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>*15 July 2005*</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12-21,23-25,27 and 28* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,12-21,23-25,27 and 28* is/are rejected.

7)☒ Claim(s) *1-10,12-18,20,21,23-25,27 and 28* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>*15 July 2005*</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

        1.☒ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date <u>*7/15/2005*</u>.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Priority

1.   Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) – (d) is

acknowledged.

The application is filed on 7/15/2005 but is a 371 case of PCT/EP04/00316

application filed 1/16/2004 and has a foreign priority application filed on 1/17/2003.

Preliminary Amendment

2.   Examiner acknowledges Preliminary Amendment for the claims filed 7/15/2005.

Applicants have amended pending claims 1 – 5, 7 – 10, 12, 14 – 18, 20 , 23 – 25 and

27 – 28 and cancelled claims 11, 22 and 26. The submitted amendments have been

entered and made of record. Presently, pending claims are 1 – 10, 12, 13 – 21, 23 –

25, 27 and 28.

Specification

3.   The disclosure is objected to because it contains an embedded hyperlink (SPEC:

Page 9 Line 11 – 12). Applicant is required to delete the embedded hyperlink and/or

other form of browser-executable code. See MPEP § 608.01.

Claim Objection

4.   Claims 1 and 5 are objected to because of the following informalities: "Method"

should be replaced with "A method". Appropriate correction(s) is (are) required.

5.   Claims 2 – 4 and 6 – 10, 12 -- 17 are objected to because of the following informalities: "Method" should be replaced with "The method". Appropriate correction(s) is (are) required.

6.   Claim 16 is objected to because of the following informalities: "bonus material of the content" should be replaced with "bonus material of a content". Appropriate correction(s) is (are) required.

7.   Claim 18 is objected to because of the following informalities: "Computer program product" should be replaced with "A computer program product". Appropriate correction(s) is (are) required.

8.   Claim 20 is objected to because of the following informalities: "Record carrier" should be replaced with "A record carrier". Appropriate correction(s) is (are) required.

9.   Claims 21, 23 – 25, 27 and 28 are objected to because of the following informalities: "Record carrier" should be replaced with "The record carrier". Appropriate correction(s) is (are) required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

10.   Claim 18 is rejected under 35 U.S.C. 101 because these claims are directed to "A computer program product", which is merely an example of functional descriptive material, (i.e. software, per se), and is nonstatutory under 35 USC 101. By not limiting

the computer program product to being stored on a computer readable storage medium,
there is a lack of the required functional and structural interrelationship between the
software and the computer storage medium that permits the functionality of the software
to be realized upon access by a processor. This ability is what underlies the ability to
provide a practical application. Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760. In
re Sarkar, 588 F.2d 1330, 1333, 200 USPQ 132, 137 (CCPA 1978). See MPEP § 2106
(IV.B).1(a).

Examiner suggests incorporating dependent claim 19 into the claim 18 to resolve
the 101 issue set forth as above.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly
claiming the subject matter which the applicant regards as his invention.

11.   Claims 4, 6 and 18 are rejected under 35 U.S.C. 112, second paragraph, as
being indefinite for failing to particularly point out and distinctly claim the subject matter
which applicant regards as the invention.

Regarding claims 4 and 6, the use of the claim language "preferably" renders
these claims indefinite, since this claim language leads to a question of whether the
claimed operations really occurred and as such merely suggests limitations or makes
limitations indefinite and optional.

Regarding claim 18, the phrase "or the like" renders the claim(s) indefinite
because the claim(s) include(s) elements not actually disclosed (those encompassed by

"or the like"), thereby rendering the scope of the claim(s) unascertainable. See MPEP

§ 2173.05(d).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12.   Claims 1 – 10, 12, 13, 15 – 21, 23 – 25, 27 and 28 are rejected under 35 U.S.C.

103(a) as being unpatentable over Paolucci et al. (Frence Patent FR-A-2822255), in

view of Rajakarunanayake (U.S. Patent 6,587,883, and in view of Greene et al. (U.S.

Patent 6,802,000).

As per claim 1, Paolucci teaches a method for **securing an access to a**

predetermined area of a target server (Paolucci: Page 5 Line 1 – 3, Page 10, 2nd Para

and Page 17, 3rd Bullet: enabling a secure access to a specific internet website (i.e. a

predetermined area of a target server) from a CD), characterized by:

providing an information file on a copy protected record carrier (Paolucci:

Page 6, 2nd Para, 1 – 4 Bullets, Page 10 Line 1 – 2, Page 16, 2nd – 5th Para, Page 17,

3rd Bullet, Page 7 Line 1 and Page 9, 1st Para / 3rd Para: a CD that stores user

information (e.g., 5 -character confidential code, URL address and password) in a

secure manner by making it <u>impossible to be reproduced</u> is considered as one type of

copy protected record carriers and the stored user information allowing a user to

automatically access and launch an internet connection request is considered as an

information file), **which information file comprises a project identifier <u>and/or</u> an**

address of an authentication server with which an application using said

information file can communicate (Paolucci: Page 7 Line 1, Page 15 Line 6 – 8, Page

17, 3rd Bullet, Page 10, 2nd Para, Page 9, 1st Para / 3rd Para, Page 14 Line 5 – 7 and

Page 6, Last 2nd Bullets: (a) the information regarding the application enabling a secure

access to a specific internet website is stored on the CD (b) the stored information to

automatically launch the internet connection request to access specific internet website

and to validate the authorized opening session with 5 characters confidential code (&

URL address and password) is considered as part of information to communicate with

an authentication server and (c) the user's confidential access code (& URL address

and password) to access a specific internet website is considered as part of a project

identifier).

However, Paolucci does not disclose expressly the authentication server can

initiate and confirm a connection between a computer on which said application is

started and said predetermined area of said target server that is identified by the

authentication server and/or the project identifier.

Rajakarunanayake teaches **the authentication server can initiate and confirm**

a connection between a computer on which said application is started and said

predetermined area of said target server that is identified by the authentication

server and/or the project identifier (Rajakarunanayake: Column 6 Line 36 – 38 / Line

50 – 53 / Line 63 – 67 and Column 12 Line 1 – 2 / Line 12 – 17 & Figure 3 / Element

330 & 157: an Authentication server is used to provide a secure connection to a secure

target location and the user identifier (i.e. authentication information) is used by the

Authentication server to uniquely identify the desired target location and once the

desired target location is determined (i.e. after the positive verification of the user

identifier and authentication information by the authentication server), a new session is

established between the user and the determined target location by the authentication

server – i.e., there are two sections: one session between the clients and the

authentication server and subsequently a new session is started between the clients

and the target system (ISP)).

    It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of Rajakarunanayake within the system of

Paolucci because (a) Paolucci teaches providing an automated secured access to a

target location (i.e. internet website) by launching of the process from a user's CD at the

client site and authenticating with the target system for the open session connection

(Paolucci : Page 2 Line 1 – 2 and Page 6, 5th Bullet), and (b) Rajakarunanayake

teaches using an authentication server to establish a new secured session between the

user and the determined target location while the connectivity is disabled to other target

locations so that the desired target system at the secure location may not be exposed to

the risk of unauthorized access (Rajakarunanayake: Column 12 Line 1 – 2 / Line 12 –

17 & Figure 3 / Element 330 & 157 and Column 2 Line 7 – 10).

Paolucci as modified does not disclose expressly said authentication server

verifies whether or not a changing parameter of the computer, in particular a randomly

generated number and/or a computer system time transmitted from said computer, was

not already previously used and initiates a connection of said computer with said

predetermined area of said target in case of a positive verification.

Greene teaches **said authentication server verifies whether or not a**

changing parameter of the computer, in particular a randomly generated number

and/or a computer system time transmitted from said computer, was not already

previously used and initiates a connection of said computer with said

predetermined area of said target in case of a positive verification (Greene:

Column 1 Line 50 – 52 / Line 55 – 60: a one-time pad of passwords is synchronously

changed and used between the end-to-end parties and a previously valid password

does not provide any information about the validity of subsequent passwords).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of Greene within the system of Paolucci as

modified because (a) Paolucci teaches providing an automated secured access to a

target location (i.e. internet website) by launching of the process from a user's CD at the

client site and authenticating with the target system for the open session connection

(Paolucci : Page 2 Line 1 – 2 and Page 6, 5th Bullet), and (b) Greene teaches using an

one-time pad of passwords to be synchronously changed between the client and the

authentication server so that exposure of a password over an insecure channel does

not compromise the security of subsequent transactions because a previously valid

password does not provide any information about the validity of subsequent passwords

(Greene: Column 1 Line 50 – 52 / Line 55 – 60).

As per claim 5, Paolucci teaches a method for **starting a secure access to a**

predetermined area of a target server (Paolucci: Page 5 Line 1 – 3, Page 10, 2nd Para

and Page 17, 3rd Bullet: enabling a secure access to a specific internet website (i.e. a

predetermined area of a target server) from a CD), characterized by:

accessing of an information file on a copy protected record carrier

(Paolucci: Page 6, 2nd Para, 1 – 4 Bullets, Page 10 Line 1 – 2, Page 16, 2nd – 5th Para,

Page 17, 3rd Bullet, Page 7 Line 1 and Page 9, 1st Para / 3rd Para: a CD that stores user

information (e.g., 5 -character confidential code, URL address and password) in a

secure manner by making it <u>impossible to be reproduced</u> is considered as one type of

copy protected record carriers and the stored user information allowing a user to

automatically access and launch an internet connection request is considered as an

information file), **which information file comprises a project identifier and/or an**

address of an authentication server with which an application using said

information file can communicate (Paolucci: Page 7 Line 1, Page 15 Line 6 – 8, Page

17, 3rd Bullet, Page 10, 2nd Para, Page 9, 1st Para / 3rd Para, Page 14 Line 5 – 7 and

Page 6, Last 2nd Bullets: (a) the information regarding the application enabling a secure

access to a specific internet website is stored on the CD (b) the stored information to

automatically launch the internet connection request to access specific internet website

and to validate the authorized opening session with 5 characters confidential code (&

URL address and password) is considered as part of information to communicate with

an authentication server and (c) the user's confidential access code (& URL address

and password) to access a specific internet website is considered as part of a project

identifier).

However, Paolucci does not disclose expressly the authentication server can

initiate and confirm a connection between a computer on which said application is

started and said predetermined area of said target server that is identified by the

authentication server and/or the project identifier.

Rajakarunanayake teaches **the authentication server can initiate and confirm**

a connection between a computer on which said application is started and said

predetermined area of said target server that is identified by the authentication

server and/or the project identifier (Rajakarunanayake: Column 6 Line 36 – 38 / Line

50 – 53 / Line 63 – 67 and Column 12 Line 1 – 2 / Line 12 – 17 & Figure 3 / Element

330 & 157: an Authentication server is used to provide a secure connection to a secure

target location and the user identifier (i.e. authentication information) is used by the

Authentication server to uniquely identify the desired target location and once the

desired target location is determined (i.e. after the positive verification of the user

identifier and authentication information by the authentication server), a new session is

established between the user and the determined target location by the authentication

server – i.e., there are two sections: one session between the clients and the

authentication server and subsequently a new session is started between the clients

and the target system (ISP)).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of Rajakarunanayake within the system of

Paolucci because (a) Paolucci teaches providing an automated secured access to a

target location (i.e. internet website) by launching of the process from a user's CD at the

client site and authenticating with the target system for the open session connection

(Paolucci : Page 2 Line 1 – 2 and Page 6, 5th Bullet), and (b) Rajakarunanayake

teaches using an authentication server to establish a new secured session between the

user and the determined target location while the connectivity is disabled to other target

locations so that the desired target system at the secure location may not be exposed to

the risk of unauthorized access (Rajakarunanayake: Column 12 Line 1 – 2 / Line 12 –

17 & Figure 3 / Element 330 & 157 and Column 2 Line 7 – 10).

Paolucci as modified does not disclose expressly said authentication server

verifies whether or not a changing parameter of the computer, in particular a randomly

generated number and/or a computer system time transmitted from said computer, was

not already previously used.

Greene teaches **said authentication server verifies whether or not a**

changing parameter of the computer, in particular a randomly generated number

and/or a computer system time transmitted from said computer, was not already

previously used (Greene: Column 1 Line 50 – 52 / Line 55 – 60: a <u>one-time pad of</u>

<u>passwords</u> is synchronously changed and used between the end-to-end parties and a

previously valid password does not provide any information about the validity of
subsequent passwords).

It would have been obvious to a person of ordinary skill in the art at the time the
invention was made to combine the teaching of Greene within the system of Paolucci as
modified because (a) Paolucci teaches providing an automated secured access to a
target location (i.e. internet website) by launching of the process from a user's CD at the
client site and authenticating with the target system for the open session connection
(Paolucci : Page 2 Line 1 – 2 and Page 6, 5th Bullet), and (b) Greene teaches using an
one-time pad of passwords to be synchronously changed between the client and the
authentication server so that exposure of a password over an insecure channel does
not compromise the security of subsequent transactions because a previously valid
password does not provide any information about the validity of subsequent passwords
(Greene: Column 1 Line 50 – 52 / Line 55 – 60).

**initiates a connection of said computer with said predetermined area of
said target server in case of a positive verification** (Rajakarunanayake: Column 6
Line 36 – 38 / Line 50 – 53 / Line 63 – 67 and Column 12 Line 1 – 2 / Line 12 – 17 &
Figure 3 / Element 330 & 157: after the positive verification of the user identifier and
authentication information by the authentication server (i.e. once the desired target
location is determined), a new session is established between the user and the
determined target location by the authentication server).

As per claim 20, Paolucci teaches **a record carrier** (Paolucci: Page 5 Line 1 – 3,

Page 10, 2nd Para and Page 17, 3rd Bullet: enabling a secure access to a specific

internet website (i.e. a predetermined area of a target server) from a record carrier CD),

characterized by:

being copy protected and comprising an application and an information file

(Paolucci: Page 6, 2nd Para, 1 – 4 Bullets, Page 10 Line 1 – 2, Page 16, 2nd – 5th Para,

Page 17, 3rd Bullet, Page 7 Line 1 and Page 9, 1st Para / 3rd Para: a CD that stores user

information (e.g., 5 -character confidential code, URL address and password) in a

secure manner by making it <u>impossible to be reproduced</u> is considered as one type of

copy protected record carriers and the stored user information allowing a user to

automatically access and launch an application process in auto-run mode from the CD

to make an internet connection request are considered as the application process and

the information file), **which information file comprises a project identifier and/or an**

address of an authentication server with which the application using said

information file can communicate (Paolucci: Page 7 Line 1, Page 15 Line 6 – 8, Page

17, 3rd Bullet, Page 10, 2nd Para, Page 9, 1st Para / 3rd Para, Page 14 Line 5 – 7 and

Page 6, Last 2nd Bullets: (a) the information regarding the application enabling a secure

access to a specific internet website is stored on the CD (b) the stored information to

automatically launch the internet connection request to access specific internet website

and to validate the authorized opening session with 5 characters confidential code (&

URL address and password) is considered as part of information to communicate with

an authentication server and (c) the user's confidential access code (& URL address

and password) to access a specific internet website is considered as part of a project

identifier).

However, Paolucci does not disclose expressly the authentication server can

initiate and confirm a connection between a computer on which said application file is

started and a predetermined area of a target server that is identified by the

authentication server and/or the project identifiers.

Rajakarunanayake teaches **the authentication server can initiate and confirm**

a connection between a computer on which said application file is started and a

predetermined area of a target server that is identified by the authentication

server and/or the project identifiers (Rajakarunanayake: Column 6 Line 36 – 38 / ·

Line 50 – 53 / Line 63 – 67 and Column 12 Line 1 – 2 / Line 12 – 17 & Figure 3 /

Element 330 & 157: an Authentication server is used to provide a secure connection to

a secure target location and the user identifier (i.e. authentication information) is used

by the Authentication server to uniquely identify the desired target location and once the

desired target location is determined (i.e. after the positive verification of the user

identifier and authentication information by the authentication server), a new session is

established between the user and the determined target location by the authentication

server – i.e., there are two sections: one session between the clients and the

authentication server and subsequently a new session is started between the clients

and the target system (ISP)).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of Rajakarunanayake within the system of

Paolucci because (a) Paolucci teaches providing an automated secured access to a target location (i.e. internet website) by launching of the process from a user's CD at the client site and authenticating with the target system for the open session connection (Paolucci : Page 2 Line 1 – 2 and Page 6, 5th Bullet), and (b) Rajakarunanayake teaches using an authentication server to establish a new secured session between the user and the determined target location while the connectivity is disabled to other target locations so that the desired target system at the secure location may not be exposed to the risk of unauthorized access (Rajakarunanayake: Column 12 Line 1 – 2 / Line 12 – 17 & Figure 3 / Element 330 & 157 and Column 2 Line 7 – 10).

Paolucci as modified does not disclose expressly said application transmits a changing parameter of the computer, in particular a randomly generated number and/or a computer system time to said authentication server so that said authentication server can verify whether or not the changing parameter of the computer was not already previously used.

Greene teaches **said application transmits a changing parameter of the computer, in particular a randomly generated number and/or a computer system time to said authentication server so that said authentication server can verify whether or not the changing parameter of the computer was not already previously used** (Greene: Column 1 Line 50 – 52 / Line 55 – 60: a <u>one-time pad of passwords</u> is synchronously changed and used between the end-to-end parties and a previously valid password does not provide any information about the validity of subsequent passwords).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of Greene within the system of Paolucci as

modified because (a) Paolucci teaches providing an automated secured access to a

target location (i.e. internet website) by launching of the process from a user's CD at the

client site and authenticating with the target system for the open session connection

(Paolucci : Page 2 Line 1 – 2 and Page 6, 5th Bullet), and (b) Greene teaches using an

<u>one-time pad of passwords</u> to be synchronously changed between the client and the

authentication server so that exposure of a password over an insecure channel does

not compromise the security of subsequent transactions because a previously valid

password does not provide any information about the validity of subsequent passwords

(Greene: Column 1 Line 50 – 52 / Line 55 – 60).

initiate a connection of said computer with said predetermined area of said

target server in case of a positive verification (Rajakarunanayake: Column 6 Line 36

– 38 / Line 50 – 53 / Line 63 – 67 and Column 12 Line 1 – 2 / Line 12 – 17 & Figure 3 /

Element 330 & 157: after the positive verification of the user identifier and authentication

information by the authentication server (i.e. once the desired target location is

determined), a new session is established between the user and the determined target

location by the authentication server).

As per claim 2, Paolucci as modified teaches characterized by providing an

autorun-information file on said record carrier, which autorun-information file provides

an automatic execution of a predetermined executable file after the record carrier is

loaded in a reading device (Paolucci: Page 7, Section of Auto-run mode, 1st Para and

Page 7 Line 1: automatic launching of connection request upon the insertion of the CD).

As per claim 3 and 25, Paolucci as modified teaches providing an autostart file

on said record carrier, which autostart file gets automatically executed after the record

carrier is placed and loaded in a reading device and which autostart file provides a link

to start said application, or which autostart file is part of said application, or which

autostart file is said information file (Paolucci: Page 7, Section of Auto-run mode, 1st

Para, Page 17, 3rd Bullet and Page 7 Line 1 and Page 15 Line 6 – 8: automatic

launching of connection request upon the insertion of the CD).

As per claim 4, Paolucci as modified teaches providing the application on said

record carrier, or on a server, preferably downloadable, or on an access-software record

carrier (Paolucci: Page 6, 2nd Para, 1st Bullet and Page 15 Line 6 – 8: Launching of the

process in Auto-run mode from the CD).

As per claim 6, Paolucci as modified teaches starting the application from said

record carrier, or from a server, preferably as a download, or via an access-software

record carrier, preferably after an installation of the application on a hard disc of the

computer (Paolucci: Page 6, 2nd Para, 1st Bullet and Page 17, 3rd Bullet: Launching of

the process in Auto-run mode from the CD).

As per claim 7, 21 and 23, Paolucci as modified teaches said application verifies

whether or not the record carrier is an original and performs said communication with

said authentication server in case of a positive verification (Paolucci: Page 10 Line 1 – 2

& 2nd Para, Page 6, Last 2nd Para, Page 9, 1st Para and Page 17, 3rd Bullet: an access

to a certain website is only possible by using the original CD because the information

file (e.g., key / confidential access code, URL and password) integrated into a specific

file enabling a secure access to the website is copy-protected (i.e. is impossible to be

reproduced)) and as such, the communication with the authentication server cannot be

started without the information file due to being copy-protected).

As per claim 8, Paolucci as modified teaches said application transmits a

changing parameter of the computer, in particular a randomly generated number and/or

a computer system time to said authentication server (Greene: Column 1 Line 50 – 52 /

Line 55 – 60: a one-time pad of passwords is synchronously changed and used

between the end-to-end parties and a previously valid password does not provide any

information about the validity of subsequent passwords).

As per claim 9, Paolucci as modified teaches said authentication server verifies

whether or not the communication with said application and/or a transmission of said

project identifier as a request for a connection between said computer and said

predetermined area of said target server is posted from said application and initiates a

connection of said computer with said predetermined area of said target server in case

of a positive verification (Paolucci: Page 7 Line 1, Page 8, 2nd Para / Line 5 – 7 Page 9,

1st Para and Page 17, 3rd Bullet: between the access device and the authentication

server) & (Rajakarunanayake: Column 12 Line 1 – 2 / Line 12 – 17 & Figure 3 / Element

330 & 157 and Column 2 Line 7 – 10: after the positive verification of the user identifier

and authentication information by the authentication server, a new session is

established between the user and the determined target location by the authentication

server).

As per claim 10, Paolucci as modified teaches after a positive verification a

connection between said authentication server and said target server is set-up by said

authentication server that connects to said target server to secure that the computer is

connected to said predetermined area of said target server via said authentication

server (Rajakarunanayake: Column 12 Line 1 – 2 / Line 12 – 17 & Figure 3 / Element

330 & 157 and Column 2 Line 7 – 10: after the positive verification of the user identifier

and authentication information by the authentication server, a new session is

established between the user and the determined target location by the authentication

server).

As per claim 12, Paolucci as modified teaches:

the authentication server generates a session identifier based on the positive

verified values and transmits said session identifier to said target server via said

connection between said authentication server and said target server

(Rajakarunanayake: Column 12 Line 1 – 2 / Line 12 – 17 & Figure 3 / Element 330 &

157 and Column 2 Line 7 – 10: after the positive verification of the user identifier and

authentication information by the authentication server, a new session is established

between the user and the determined target location by the authentication server),

said connection between said computer on which said application is started and

said predetermined area of said target server is set up by redirecting the connection

between the computer and the authentication server to the target server or by

forwarding data of the protected area to the computer (Rajakarunanayake: Column 12

Line 1 – 2 / Line 12 – 17 & Figure 3 / Element 330 & 157 and Column 2 Line 7 – 10),

and

said connection between said computer on which said application is started and

said predetermined area of said target server is executed after the target server

received a confirmation of a validity of the session identifier from the authentication

server (Rajakarunanayake: Column 6 Line 63 – Column 7 Line 1 and Column 12 Line 1

– 2 / Line 12 – 17: when the user ends the session to the target location, the user need

to be authenticated by the authentication server again – and therefore, Examiner notes

the target server received a confirmation of a validity of the session identifier from the

authentication server).

As per claim 13, Paolucci as modified teaches the authentication server confirms

the validity of the session identifier by positively determining whether or not the session

identifier exists and/or whether or not the session identifier was already requested to be

valid (Greene: Column 1 Line 50 – 52 / Line 55 – 60: a one-time pad of passwords is synchronously changed and used between the end-to-end parties and a previously valid password does not provide any information about the validity of subsequent passwords).

As per claim 15, Paolucci as modified teaches said record carrier is copy protected by copy protecting the information file (Paolucci: Page 10 Line 1 – 2 & 2nd Para, Page 6, Last 2nd Para, Page 9, 1st Para and Page 17, 3rd Bullet: key / confidential access code, URL and password integrated into a specific file, as part of the information file, enabling a secure access to an internet website is <u>copy-protected</u> (i.e. is <u>impossible to be reproduced</u>), as taught by Paolucci).

As per claim 16 and 28, Paolucci as modified teaches said predetermined area on said target server comprises bonus material of the content that is included on the record carrier besides said executable file (Paolucci: Page 19 Last Para, Page 18 Last 2nd Para: e.g. a email address search list or an international phone book is considered as a bonus material included in the predetermined email URL address website).

As per claim 17 and 27, Paolucci as modified teaches said information file is a part of said application or is an executable file of said application (Paolucci: Page 10 Line 4 – 6 / Line 10 – 11, Page 17, 3rd Bullet and Page 14 Line 6 – 7).

As per claim 18, Paolucci as modified teaches computer program means adapted to perform the method steps as defined in claim 1 or parts thereof when being executed on a computer, digital signal processor, or the like (Paolucci: Page 2 and Page 5).

As per claim 19, Paolucci as modified teaches computer readable storage means, comprising a computer program product according to claim 18 (Paolucci: Page 2 and Page 5).

As per claim 24, Paolucci as modified teaches an autorun-information file, which provides an automatic execution of a predetermined executable file after the record carrier is loaded in a reading device (Paolucci: Page 7, Section of Auto-run Mode, Line 1 – 4: loaded from a CD reader as a reading device).

13.   Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Paolucci et al. (Frence Patent FR-A-2822255), in view of Rajakarunanayake (U.S. Patent 6,587,883, and in view of Greene et al. (U.S. Patent 6,802,000), and in view of Mitchell et al. (U.S. Patent 6,959,420).

As per claim 14, Paolucci as modified does not disclose expressly the target server assigns a temporary session cookie to the computer so that the whole

predetermined area of the target server can be accessed via said connection between

said computer on which said application is started and said target server.

Mitchell teaches the target server assigns a temporary session cookie to the

computer so that the whole predetermined area of the target server can be accessed

via said connection between said computer on which said application is started and said

target server (Mitchell: Column 1 Line 28 – 35 / Line 43 – 45 / Line 56 – 60: a temporary

or session cookie is stored on a user's computer only for the current browsing session

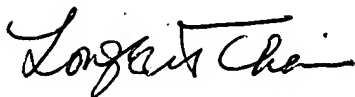and the cookie is deleted from the computer when the browsing software is closed).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of Greene within the system of Paolucci as

modified because (a) Paolucci teaches providing an automated secured access to a

target location (i.e. internet website) by launching of the process from a user's CD at the

client site and authenticating with the target system for the open session connection

(Paolucci : Page 2 Line 1 – 2 and Page 6, 5th Bullet), and (b) Mitchell teaches using a

temporary session cookie to be stored on a user's computer so that the user does not

have to repeatedly resubmit information to the website and the cookie is valid only for

the current browsing session and is deleted when the browsing session is closed to

avoid the abuse of the user's privacy by the untrustworthy website (Mitchell: Column 1

Line 28 – 35 / Line 43 – 45 / Line 56 – 60 / Line 61 – 67).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai, Ph.D.
Patent Examiner
Art Unit 2131
4/27/2007